AMENDMENTS TO THE CLAIMS

Pursuant to 37 C.F.R. § 1.121 the following listing of claims will replace all prior versions, and listings, of claims in the application.

1 – 2. (Canceled)

3. (withdrawn) A method for establishing a common key for a group of at least three subscribers, the method comprising:
generating by each subscriber Ti of the at least three subscribers a respective message $Ni = (g^{zi} \bmod p)$ from a publicly known element g of large order of a publicly known mathematical group G and a respective random number zi and sending the respective message from the respective subscriber to all other subscribers Tj of the at least three subscribers, each respective random number zi being selected or generated by the respective subscriber Ti;
generating by each subscriber Ti a transmission key k^{ij} from the messages Nj received from the other subscribers Tj, $j \neq i$, and the respective random number zi according to $k^{ij}: = Nj^{zi} = (g^{zj})^{zi}$;
sending by each subscriber Ti the respective random number zi in encrypted form to all other subscribers Tj by generating the message Mij according to $Mij := E(k^{ij}, zi)$, $E(k^{ij}, zi)$ being a symmetrical encryption algorithm in which the data record zi is encrypted with the transmission key k^{ij}; and
determining a common key k by each subscriber Ti using the respective random number zi and the random numbers zj, $j \neq i$, received from the other subscribers according to
$k: = f(z1, ..., zn)$,
f being a symmetrical function which is invariant under a permutation of its arguments.

4. (withdrawn) The method as recited in claim 3 wherein the transmission key k^{ij} is known to subscriber Tj according to $k^{ij} = k^{ji}$.

5. (Currently Amended) A method for establishing a common key for a group of at least three subscribers for transmitting messages over a communication channel, the method comprising the steps of:

generating, by each subscriber T_j, a respective message ~~$N_i := (g^{zi} \bmod p)$~~ $N_j = (g^{zj} \bmod p)$ from a publicly known element g of large order of a publicly known mathematical group G and a respective random number [[zi]] zj, j = 1 to n, where n is the number of subscribers in the group of at least three subscribers; ~~and~~

sending the respective message, by each subscriber except a predetermined first subscriber T_1 of the at least three subscribers, to the first subscriber T_1~~, each respective random number [[zi]] being selected or generated by the respective subscriber [[Ti]]~~;

encrypting, by the first subscriber T_1, the received messages N_j of the other subscribers T_j, $j \neq 1$, with the random number z1 to form a respective transmission key k^{1j} for each subscriber T_j, $j \neq 1$;

sending, by the first subscriber T_1, the random number z1 to all other subscribers T_j, $j \neq 1$ in encrypted form by generating a message M_{1j} according to $M_{1j} := E(k^{1j}, z1)$, $E(k^{1j}, z1)$ being a symmetrical encryption algorithm in which the random number z1 is encrypted with the transmission key k^{1j}; and

determining a common key k, by each subscriber [[T_i]] Tj, ~~using the values Ni and Nj, $j \neq i$, and the random number z1 sent by the first subscriber T1 in encrypted form~~ using an assignment $k := h(z1, g^{z2}, ..., g^{zn})$, h (x1, x2, ..., xn) being a function which is symmetrical in the arguments x2, ..., xn, the common key k being useable for transmitting messages over a communication channel.

6. (Currently Amended) The method as recited in claim 5 wherein the transmission key is known to subscriber T_j according to $k^{1j} = k^{j1}$.

7. (New) A method for establishing a common key for a group of subscribers for encryption and decryption of messages, the method comprising the steps of:

each of the subscribers T_j generating a respective random number zj, where j goes from 1 to n and n is the number of subscribers in the group of subscribers;

each of the subscribers T_j generating a respective first message N_j = (g^{zj} mod p) from a publicly known element g of large order of a publicly known mathematical group G;

each of the subscribers T_j, $j \neq 1$, sending the respective first message to a first subscriber T_1;

the first subscriber T_1 computing a transmission key $k^{1j} = N_j^{z1}$ mod p for each of the other subscribers T_j, $j \neq 1$, based on the received respective first message N_j, $j \neq 1$;

the first subscriber T_1 encrypting a second message $M_{1j} := E(k^{1j}, z1)$ for each of the other subscribers T_j, $j \neq 1$, where $E(k^{1j}, z1)$ is a symmetrical encryption algorithm in which z1 is encrypted with the transmission key k^{1j};

the first subscriber T_1 sending the encrypted second message M_{1j} to each of the other subscribers T_j, $j \neq 1$; and

each of the subscribers T_j computing a common key k according to an assignment k:=h(z1, g^{z2}, … g^{zn}), where h(x1,x2…xn) is a symmetrical function.

8. (New) The method according to claim 7, wherein the respective random number zj is selected from the set {1, . . . p-2}.

9. (New) The method according to claim 7, wherein the length of p is at least 1024 bits.

10. (New) The method according to claim 7, wherein g has a multiplicative order of at least 2^{160}.

11. (New) The method according to claim 7 wherein the transmission key is known to a respective subscriber Tj according to $k^{1j} = k^{j1}$.

12. (New) The method according to claim 7, wherein $h(z1, g^{z2}, \ldots g^{zn}) = g^{z1*z1} * g^{z2*z1} * \ldots g^{zn*z1}$.

13. (New) A method for establishing a common key for a group of subscribers for encryption and decryption of messages, the method comprising the steps of:

each of the subscribers T_j generating a respective random number zj, where j goes from 1 to n and n is the number of subscribers in the group of subscribers;

each of the subscribers T_j storing the respective random number zj in a respective memory;

each of the subscribers T_j generating a respective first message $N_j = (g^{zj} \bmod p)$ from a publicly known element g of large order of a publicly known mathematical group G;

each of the subscribers T_j, $j \neq 1$, sending the respective first message to a first subscriber T_1;

the first subscriber T_1 storing each of the received first messages in a memory;

the first subscriber T_1 computing a transmission key $k^{1j} = N_j^{z1} \bmod p$ for each of the other subscribers T_j, $j \neq 1$, based on the received respective first message N_j, $j \neq 1$;

the first subscriber T_1 encrypting a second message $M_{1j} := E(k^{1j}, z1)$ for each of the other subscribers T_j, $j \neq 1$, where $E(k^{1j}, z1)$ is a symmetrical encryption algorithm in which z1 is encrypted with the transmission key k^{1j} ;

the first subscriber T_1 sending the encrypted second message M_{1j} to each of the respective other subscribers T_j, $j \neq 1$;

each of the respective other subscribes T_j, $j \neq 1$, storing the received encrypted second message in the respective memory; and

each of the subscribers T_j computing a common key k according to an assignment $k:=h(z1, g^{z2}, \ldots g^{zn})$, where $h(x1,x2\ldots xn)$ is a symmetrical function, and n is the number of subscribes in the group.

14. (New) The method according to claim 13, wherein a maximum number of transmission rounds required is two.

15. (New) The method according to claim 13, further comprising the steps of:

one of the respective subscribers T_i using the computed common key k to encrypt a third message;

the one of the respective subscribers T_i transmitting the encrypted third message to each of the other respective subscribers;

each of the other respective subscribers T_j, $j \neq i$ decrypting the received encrypted third message using the computed common k.